POL – Information Security Policy

Appendix C

Table of Contents

I. Blocked Internet Sites

Web Site Filters
Last Update: 09/3/2014

This appendix identifies the individual and classes of web sites that are filtered by the Department of Administration, Information Technology Services Division. The sites or classes of sites filtered affect all devices connected to SummitNet and are subject to change at any time with the approval of the State of Montana, Chief Information Officer.

Adult Material

Adult Content Lingerie and Swimsuit Nudity
Sex

Bandwidth

Entertainment Video Internet Radio and TV Internet Telephony
Peer-to-Peer File Sharing
Personal Network Storage and Backup Surveillance
Viral Video

Entertainment

Media File Download

Extended Protection

Dynamic DNS Elevated Exposure Emerging Exploits
Suspicious Content

Gambling Games

Illegal or Questionable

Information Technology

Hacking
Proxy Avoidance
Web and Email Spam Website
Translation

Internet Communication

General Email
Text and Media Messaging Web Chat

Intolerance Parked

Domain Productivity

Advertisements Instant
Messaging Pay-to-Surf

Security

Advanced Malware Command and Control Advanced
Malware Payloads
Bot Networks Compromised Websites
Custom-Encrypted Uploads Files
Containing Passwords Keyloggers
Malicious Embedded iFrame Malicious
Embedded Link Malicious Web Sites
Mobile Malware
Phishing and Other Frauds Potentially
Exploited Documents Potentially Unwanted
Software Spyware
Suspicious Embedded Link

Social Web-Facebook

Facebook Games Facebook Mail

Social Web-Twitter

Twitter Mail

Society and Lifestyles

Personal and Dating

Tasteless Violence

State of Montana Default Protocol restrictions:

Instant Messaging/Chat

AOL Instant Messenger or ICQ Baidu Hi
Brosix Camfog
Chikka Messenger Eyeball
Chat Gadu-Gadu Gizmo
Project Globe7
Gmail Chat (WSG Only) Goober
Messenger Google Talk
IMVU IRC
iSpQ Mail.Ru Meetro
MSC Messenger MSN
Messenger MySpaceIM
NateOn
Neos Netease Popo
netFM Messenger
Nimbuzz Palringo
Paltalk
SIMP (Jabber) Tencent QQ
TryFast Messenger
VZOchat
Wavago Wengo
Woize Xfire
X-IM
Yahoo! Mail Chat Yahoo!
Messenger

Instant Messaging File Attachments

AOL Instant Messenger or ICQ attachments MSN
Messenger attachments
NateOn Messenger Attachments Yahoo!
Messenger attachments

Mail and Collaborative Tools

IMAP
Microsoft HTTPMail

Malicious Traffic

Bot Networks

P2P File Sharing

Ares
Badongo Buddy
BitTorrent BoxCloud
ClubBox Damaka
DirectConnect eDonkey
EZPeer
FastTrack (Kazza iMesh)
FolderShare
Giga Tribe
Gnutella (Morpheus Xolox) Google
Wave (WSG Only) Hamachi
Hotline Connect Live
Mesh MindSpring
Onshare Opera Unite
Orsiso
Pando Project Neon
Qnext Raketu
ShareNow Skype
Solid State Delivery Platform SoulSeek
VoxOx

Proxy Avoidance

GhostSurf
Google Web Accelerator Hopster
JAP
RealTunnel SocksOnline
TongTongTong Toonel
Tor
Your Freedom

Remote Access

Access Grid
BelnSync
Comodo Easy VPN CrossLoop
Instant Housecall LogMeIn
Mikogo MyGreenPC
MyIVO
NateOn Remote Access
PCAnywhere pcTELECOMMUTE
SoftEther PacketiX SoonR
ssh TeamViewer
Telnet
Terminal Services VNC
Vyew WallCooler VPN
WebEx (PCNow & Support Center) Yuuguu
Zolved

System

Daytime Finger
SOCKS 5

II. Rules of System Usage

All State employees or contractors with the State who have access to the Internet, email, or other online services, will sign a consent form indicating that they have knowledge of the state's policies and procedures in regards to the use of state computing resources. Privacy in using the state's computer systems is not guaranteed. Therefore, employees should not have any expectations of privacy when using the Internet, email, or other computer services. The following is an example consent form that agencies can use for employees and contractors. Both employees and contractors shall read and sign a consent form every year.

Rules of System Usage Sample Acknowledgement Form

I _____ have read the (***Add Agency***) policies and procedures regarding the use of information systems and I agree to comply with all terms and conditions. I agree that all information system activity conducted while doing (***Add Agency***) business and being conducted with (***Add Agency***) resources is the property of the State of Montana.

I understand that any information system to which I have access, can only be used for its intended purpose. I also agree to avoid the disclosure of any protected data to which I have access.

I understand that (***Add Agency***)/SITSD reserves the right to monitor and log all information system activity including email and Internet use, with or without notice, and therefore I should have no expectations of privacy in the use of these resources.

If my position requires a background check, I understand that the results of this background check can affect my employment.

_____ Yes, this position requires a background check

_____ No, this position does not require a background check.

Signed _____

Position Title _____ Position Number _____

Date _____

*NOTE: This form will be signed by each (**Add Agency**) employee on an annual basis.*

III. Elevated Privileges Sample Acknowledgement Form

Rules of System Usage for Users with Elevated Privileges Sample Acknowledgement Form

A. INTRODUCTION

I _____, understand that I have additional responsibilities given my elevated computer access privileges. I have received training emphasizing the effects my actions can have on all information system activity. Because of these responsibilities, I understand the need for reading and signing this Acknowledgement.

B. FEDERAL AND STATE TAX INFORMATION

I understand the following:

1. I may have access to Federal Tax Information (FTI) and State Tax information as defined in footnote 1 below.
2. That tax returns or tax information disclosed to each user can be used only for a purpose and to the extent authorized by the data manager in connection with the processing, storage, transmission and reproduction of tax returns and return information, the programming, maintenance, repair, testing, and procurement of equipment, and providing of other services for purposes of tax administration.
3. That further disclosure of any tax returns or tax information for a purpose or to an extent unauthorized by the data manager for these purposes constitutes a felony, punishable upon conviction by a fine of as much as $5,000, or imprisonment for as long as five years, or both, together with the costs of prosecution (IRC 7213).
4. That further inspection of any tax returns or tax information for a purpose or to an extent not authorized by the data manager for these purposes constitutes a misdemeanor, punishable upon conviction by a fine of as much as $1,000, or imprisonment for as long as one year, or both, together with costs of prosecution (IRC 7213A)
5. That should either unauthorized access or disclosure occur, individually I can be sued by the taxpayer and would be liable for civil damages amounting to a minimum of $1,000 for each act or the actual damages sustained by the taxpayer (whichever is greater) as well as the costs of the court action (IRC 7431).
6. That under Montana law, 15-30-303 MCA, 15-70-209 MCA, 15-70-344 MCA, 15-70-351, MCA, a user cannot disclose or disseminate information contained in a statement required under the fuel tax sections. Making an unauthorized disclosure or unauthorized inspection of information can make the person subject to the progressive disciplinary procedures set out by state law which could include termination from employment.
7. I have received awareness training and understand the policies and procedures for safeguarding FTI and the penalties for unauthorized inspection or disclosure of FTI.

C. CRIMINAL JUSTICE INFORMATION

I understand the following:

1. I may have access to criminal justice information as defined in footnote 2 below, via the state network.
2. My access to this information is limited for the purpose(s) outlined in the agreement between the State Information Technology Services Division and the government agency providing the information.
3. Criminal history information and related data are particularly sensitive and may cause great harm if misused.
4. Misuse of the system by accessing it without authorization, exceeding the authorization, using the system improperly, or using, disseminating or re-disseminating criminal justice information without authorization, may constitute a state crime, federal crime, or both.

D. OTHER CONFIDENTIAL INFORMATION

I understand that I may have access to other confidential information such as a person's first and last name, address, telephone number, email address, social security number, bank and credit card information, health information, and other unique identifying information about a person. This information is confidential and may not be used or disclosed without proper authorization from my supervisor.

I have read and understand this Acknowledgement. A violation of the above terms and conditions may result in disciplinary action up to and including termination from employment.

Signed _____

Date _____

1. **FTI (IRS Code) -** A taxpayer's identity, the nature, source, or amount of his income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies over assessments, or tax payments, whether the taxpayer's return was, is being, or will be examined or subject to other investigation or processing.
2. **CJIS Data -** data considered to be criminal justice in nature to include images, files, records, and intelligence information. FBI CJIS data is information derived from state or Federal CJIS systems.